Survey on Efficient Key Pre-Distribution Scheme for Wireless Sensor Network

Jeenyta Desai[1] Indr Jeet Rajput[2]
[1]Student [2]Faculty
[1,2]Department of Computer Engineering
[1,2]Hasmukh Goswami College of Engineering, Vahlal, Ahemdabad, Gujarat, India

Abstract— Various hardware platforms have already been designed to test the many ideas spawned by the re-search community and to implement applications Wireless Sensor Networks is growing day by day and also its Security is a burning issue. at the same time, offer numerous challenges energy constraints, size of hardware, computational cost and power utilization to which sensing nodes are typically subjected. And for security, Key Management is a challenging issue. Key pre-distribution schemes are evolved in order to achieve performance. The security requirements like Global connectivity, Local Connectivity, Resiliency Key Sharing Probability and Network Scalability are to be Surveyed. A wireless sensor network (WSN) has important applications such the use of sensor networks was first limited to Military applications only but now it has its wings spread over civilian applications such as Health monitoring, Industries, environmental sensing, target tracking, wild life monitoring and communications on commercial scale and also remote environmental monitoring. Result is the availability, particularly in recent years, of sensors that are smaller, cheaper, intelligent and faster. Since Wireless Sensor Networks have become popular in recent past. A lot of research has been carried out in this field to improve hardware specifications, protocols for communications and information security. The goal of our survey is to present a comprehensive review of the recent literature on the protocols and the constrains which they are effecting. Gathering information for the protocols working and survey on how they are improved than the others and which factors are to altered to further improve them. We are so, giving a survey on the protocols used for security and the factor they effect.

***Key words*:** Connectivity, Resiliency, WSN, constraints

I. INTRODUCTION

The main fundamental of WSN is the low power tiny sensor nodes. These sensor nodes get the useful information from the environment like pressure, light, temperature, vibrations, sounds, marking, motion and then to process this information. The sensor nodes are usually moved in the sensor field. Each of the moved sensor node has the capabilities to collect data and route data back to the sink node and to the users via internet. Base station is centralized point of control within the WSN. Which extract the information from the network and disseminates control information back to the network. It also used as a Gateway to the other networks, As far as Hardware concern the base station is either laptop or a workstation [1]. All these sensor nodes are arbitrarily distributed in the network, so the basic issue is that whatever information has to be passed among nodes face the problem of security, computing and communications, which are making this emerging technology a reality.

II. OVERVIEW OF KEY ISSUES

Current state-of-the-art sensor technology has paved us a way to the varied applications in wireless sensor networks. WSN is a Network humped with many constraints as when compared to the conventional Computer networks. Our hands were not tied in traditional networks to employ the security mechanism, which in contrast is difficult to be done in case of Wireless Sensor Networks. Therefore to maintain the security mechanisms we will borrow some ideas from the traditional security techniques when needed. For this it is necessary to understand the obstacles of sensor security.

Limited resources- in terms of Memory and Storage spaces, Power Limitations, Unreliable communication- in terms of, problems in transfers, conflicts and multi-hopping, Unattended operation[6]- in terms of physical attacks, no central point management. When these issues will be taken care of while design issues then automatically the security requirements will be satisfied.

The above mentioned key issues are followed with the Security Requirements. The security requirements of the wireless sensor network can be classified as:
Availability- Surety that the service offered by the whole WSN by a part of it or by one sensor node must be available whenever required.

- Authenticity- Adversary can easily inject messages so the receiver needs to be confirming that the data used and send by it comes from the trusted sender. That is the sender and receiver must be sure that they are talking to the node to which they want to communicate.
- Confidentiality-The message on the channel will not be read and hence the message on the channel needs to be encrypted.
- Integrity-Verification of the authenticated message, that the send message is not altered by the adversary
- Scalability- If the size of the network grows than it should not compromise nodes; it should not increase communication overhead. It should allow nodes to be added after the network deployment
- Non-Reputation- It is the method of granting message transmission between parities with the ability to prevent a identified node from repudiating a specific communication associated with the other node and Hence decreasing the network overheads.

There are different security threats in wireless sensor networks like Jamming attack, Tampering attack, Collision, Exhaustion, Sink hole attack, Worm holes and Hello flood attack. Wireless sensor networks are vulnerable to security attacks due to the broad cast nature of the transmit ion medium [4].

In addition to these general requirements, Wireless Sensor Networks have following specific requirements:

- Survivability- It is An ability to provide a service even in the presence of power loss, failures or attacks
- Degradation of security services - The ability to change security level as resource availability changes

While using the Key Cryptography, there are two ways of cryptography. One is Symmetric key cryptography and the other is the Public Key Cryptography. Selection of a suitable security scheme is critical in wireless sensor networks (WSNs) because of the open media broadcast communication and the limited energy supply of the sensor device [2]. To achieve the security requirements, several researchers have focused on evaluating cryptographic algorithms in WSNs and proposing energy efficient ciphers. Although the transmission of data is the most energy consuming activity in a wireless sensor node, it is also important to select an energy efficient cipher that will minimize the energy consumption of the energy constrained sensor node. The energy efficiency of symmetric key cryptographic algorithms applied in wireless sensor networks (WSNs) and in our study we consider both stream ciphers and block ciphers. We derive the computational energy cost of the ciphers under consideration by comparing the number of CPU cycles required to perform encryption. After evaluating a number of symmetric key ciphers, we compare the energy performance of stream ciphers and block ciphers [3].

A. *Symmetric Key Cryptography:*

same key is use for both encryption and decryption of data. Algorithm used for this is easy to implement and required limited computation power for encryption and decryption .Problem is all participant node agree on same key. So this scheme is more vulnerable. and many attack like eavesdropping and capture attack is possible. Below describe the keying model of Symmetric cryptography.

B. *Public Key Cryptography:*

Problem of symmetric key is how to send a key to solve the problem public key is come. Public key cryptography was invented in seventies years. In this cryptography two key are use to encrypt and decrypt of data. Any message or data encrypted with one of the keys can only be decrypted with the other key. In Two key one key is private and another is public key private key is known by only itself node which it hold, and the second one is publicly known by each node in a given community this ensure confidentiality, integrity and authentication. But While using them in the Sensor nodes which have very less storage and computational overheads it is not possible to run the complex algorithms on every node.

III. RELATED WORK AND ANALYSIS

Key management has become a challenging issue in the design and deployment of secure wireless sensor networks. Key management is a fundamental cryptographic primitive upon which other security primitives are built. Basically, key management includes two aspects: key distribution and key revocation. Key distribution refers to the task of distributing secret keys between communicating parties to provide secrecy and authentication. Key revocation refers to the task of securely removing compromised keys. By revoking all of the keys of a compromised sensor node, the node can be removed from the network. Compared to key distribution, key revocation has received very little attention. In this paper, we have discussed several existing methods for key revocation.

Key distribution is an important issue in wireless sensor network (WSN) design. It is a newly developing field due to the recent improvements in wireless communications.

Wireless sensor networks are networks of small, battery-powered, memory-constraint devices named sensor nodes, which have the capability of wireless communication over a restricted area. Due to memory and power constraints, they need to be well arranged to build a fully functional network.

Key pre-distribution is the method of distribution of keys onto nodes before deployment. Therefore, the nodes build up the network using their secret keys after deployment, that is, when they reach their target position. Key pre-distribution schemes are various methods that have been developed by academicians for a better maintenance of key management in WSNs. Basically a key pre-distribution scheme has 3 phases:

[1] Key Distribution
[2] Shared key discovery
[3] Path-Key establishment

Right before the deployment of the network setup, the keys are to be distributed to the nodes in the network; therefore all nodes can use their own keys for the secure communication between the nodes. Once the secret keys are generated and delivered to the nodes one sensor node searches the other sensor nodes for the secure connection and this is called Shared key discovery. Thereafter, secure link is established and the connection between the nodes is accomplished.

IV. ALGORITHMS BASED ON PRE-KEY DISTRIBUTION

A. *Eschenauer and Gligor [7]:*

Eschenauer and Gligor has given the probabilistic key pre-distribution method. In most of papers this scheme is referred as basic scheme. In this approach, three phases are needed to set up the secret keys between sensor nodes. These phases are key pre distribution, shared key discovery and path key establishment. In first phase each sensor node randomly assigned different keys from a big key pool.

Stored keys in each sensor node are called key ring of the node and each key has a corresponding id. Next two phases are done when nodes are deployed. In the shared key discovery phase nodes find the common key between them and establish a secure connection. In this phase each node discovers its neighbors in communication range with which it shares common keys. It might happen that nodes are in communication range but do not share any keys, these nodes may be connected by one or more hops links through path key establishment phase. The path key establishment phase assigns a path key to the sensor nodes via one node to other and then they can set up secure link between them. Most of the pre-distribution schemes are based on this model.

In wireless sensor network base station is known as centralized authority. Base station is used to revoke the

compromised nodes. Eschenauer and Gligor presented a key management scheme for wireless sensor network in [7]. It is a centralized key revocation scheme. If a node is compromised, the base station can send a message to all other sensors to revoke the compromised node's key ring. The revocation scheme can be divided into three phases: signature key distribution, key revocation and link reconfiguration.

B. Zhang et al. Scheme [5]:

Zhang et. Al. proposed a key revocation scheme which is known as GPSRRev scheme [9]. This scheme is also a centralized key revocation scheme.

The revocation area is divided into sub-areas if the revocation area is large. Using GPSR protocol, a revocation message is sent to a certain node within each area [10]. After that for remaining sub-areas the revocation message is multicast. The revocation message includes two things: first the identifier of the sensor nodes to be revoked and the scope of the revocation area. If the sensor node is within the revocation area indicated by the revocation message, the sensor node records the identifier of the revoked sensor node and rebroadcast the message to its neighboring nodes. The message is dropped if it is outside the revocation area.

C. Chan et al. scheme:

Chan proposed a distributed key revocation scheme for sensor networks in [11] and further investigated this scheme in [12]. In this scheme, a vote is cast and collected among sensor nodes. If the vote tally against a sensor node exceeds a specified threshold, the sensor node will be revoked. In this scheme, first at the connection time neighboring nodes exchange the masks to decrypt the votes. Then in the current session, at least *t* sensor nodes cast their votes against the target node. In the next session, the voting nodes cast their votes against the target node. The compromised sensor node information needs to be broadcasted in the network if and only if a sensor node receives at least t revocation votes. Chan's scheme is built on some simplifying assumptions, such as each node knows its neighboring nodes and each node knows its neighboring node's neighboring nodes before deployment. It is hard to satisfy this requirement. The distributed key revocation scheme is faster compared with the centralized key revocation because it requires local broadcast. However, the distributed key revocation scheme is more complex than the centralized key revocation scheme. Detail information about the distributed key revocation scheme is included in [11-12].

D. Novel Deterministic Key Pre-distribution Scheme[8]:

In this scheme the pre distribution keys to each sensor nodes is done so that each sensor nodes can get common keys (kab=kba) in between the nodes Na and Nb. In the next step two separate communication links are established between the nodes. If one of the link fails to communicate or get effected by the adversary then the other node at least can do the secure communication.

The second step is to select the pool of secret keys and the secret information Sa and Sb. To compute kab and kba which is a common key between Na and Nb nodes.

The main idea is to use the two communication links so that if one fails the use of other communication can be done between two nodes. The proposed scheme is more resilient against the nodes capture but also the computational overhead increases. Fault tolerance, scalability and power consumption are some faced issues in this scheme.

E. Unital based Key Distribution[13]:

The interest here is scalability of symmetric key pre-distribution schemes. Existing research works either allow supporting a less number a nodes or degrading the other network performances in terms of resiliency, connectivity and storage overhead**.** In contrast to these solutions, our goal is to enhance the scalability of WSN key management schemes without degrading significantly the other network performances. To achieve this goal, first time, the unital design was used to construct and pre-distribute key rings.

In Unital Design: X is the point set; blocks-b are generated; total number of generated blocks-b= $m^2(m^2-m+1)$
In Key distribution: S is the key pool and $S=m^3+1$; KRi is the key ring; Total number of generated key rings-n= $m^2(m^2-m+1)$.

Set of m^3+1 point arranged in the subset of size (m+1) where U={ m^3+1,…….}subset of{m+1,……}.So that every pair of distinct points of set are contained in exactly one subset.
m={1,2,3……}then U={2,9,65,…….}subset of {2,3,4…….}
Unital is a 2-(m^3+1,m+1,1)block design.

Where m^3+1 is the key pool, m+1 is key ring size for n nodes. By using this theory the key sharing probability comes out to be $Pc = (m+1)^2/(m^3+m+1)$
However this naïve solution degrades the key sharing probability to O(1/k)….

Henceforth, unital Theory is an approach of mapping of the keys so that the network scalability increases, also the proposed scheme is the establishment of unique secrete pair wise keys between the connected nodes. However network resilience is not always ensured. As well as the key sharing probability is also less. Ahead of this after the basic use of unital design there is a proposal of a solution which ensures network scalability while maintaining good probability of key sharing.

V. CONCLUSION

Looking towards all the algorithms for the Key Pre Distribution, there are certain things which are to considered in the whole scenario while building a network. It should have all types of constraints satisfied. The performance constraints like network scalability, Resiliency, Confidentiality, Authenticity and Good Key sharing probability are all to be considered and controlled along with the problem of tiny low storage, Power limited sensor nodes. The above algorithms and many more strategies are set to be having some benefits for network building but along with those benefits there are bitter consequences also. If we consider Eschenauer and Gligor's probabilistic key sharing strategy, it serves with simplicity but has the problem of network scalability. As soon as the size of the network increases, directly the size of the key pool will have to be increased also leading to storage overhead. Similarly Chan's scheme is based on vote cast system and is built on simple assumption which states that each node should be knowing its neighboring nodes before deployment. It is hard

to satisfy this requirement and proves a hamper. Zhang proposed a centralized key revocation scheme, in which if a message is dropped outside the revocation area no communication can be established and thus ultimately giving failure to availability. In Novel deterministic key pre distribution scheme the constrain of resilience to extant is solved leaving a very important business aspect of scalability un-served. Ahead in case of Unital Theory approach where we get the maximum benefits of the network scalabilty, and the unique key distribution, then the factor like the network resiliency and enhanced key sharing probability are disturbed. Hence we need such a scheme which along with scalability, resiliency, good key sharing probability and with the redeuced storage overheads should be designed.

REFRENCES

[1] A Survey on Cryptography and key distribution in Wireless Sensor Network with Security Attack and Challenges | ISSN: 2321-9939
[2] Y. Wang, G. Attebury, B. Ramamurthy, "A Survey of Security Issues in Wireless Sensor Networks," IEEE Communications Surveys & Tutorials,vol.8, no.2, pp. 2-23, 2006
[3] Energy Efficiency of Symmetric Key CryptographicAlgorithms in Wireless Sensor Networks Xueying Zhang, Howard M. Heys,and Cheng Li Faculty of Engineering and Applied Science Memorial University of Newfoundland St. John's, NL, A1B 3X5, Canada.
[4] Monika roopak et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 25-31
[5] International Journal of Application or Innovation in Engineering & Management (IJAIEM)Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 2, February 2013 ISSN 2319 – 4847
[6] Security in Distributed, Grid, and Pervasive Computing Yang Xiao,(Eds.) pp. – - – °c 2006 Auerbach Publications, CRC Press
[7] Zhang W, Song H, Zhu S, Cao G. Least privilege and privilege deprivation: towards tolerating mobile sink compromises in wireless sensor networks. In *MobiHoc '05: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. ACM Press: New York, NY, USA, 2005; 378–389.
[8] International Journal of Advanced Research in Computer Science and Software Engineering. Novel Deterministic Key Pre-Distribution Schemes for wireless sensor networks. Volume 3,Issue 7, July 2013. ISSN:2277128X
[9] Karp B, Kung HT. GPSR: greedy perimeter stateless routing for wireless networks. In MobiCom '00: Proceedings of the6th Annual International Conference on Mobile Computing and Networking. ACM Press: New York, NY, USA, 2000; 243–254.
[10] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, CA, USA, May 2003, 197–213
[11] Chan H, Gligor V, Perrig A, Muralidharan G. On the distribution and revocation of cryptographic keys in sensor networks. *IEEETransactions on Dependable and Secure Computing* 2005; **2**(3):233–247.
[12] O. Kachirski and R. Guha, "Effective intrusion detection uses multiple sensors in wireless ad hoc networks," in System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference.
[13] Unital Design based key pre-Distribution Scheme for Wireless Sensor Networks. International Journal of Innovation research in Science, Engineering and Technology Volume 3, Special issue 3, March 2014.

